Coupling of company and machine networks

SIMOTION

Frequently asked Questions

SIEMENS

Safe connection of a machine network with SCALANCE S602

Table of Contents

Subject to change without prior notice.

Safe connection of a machine network with SCALANCE S602

1 Question

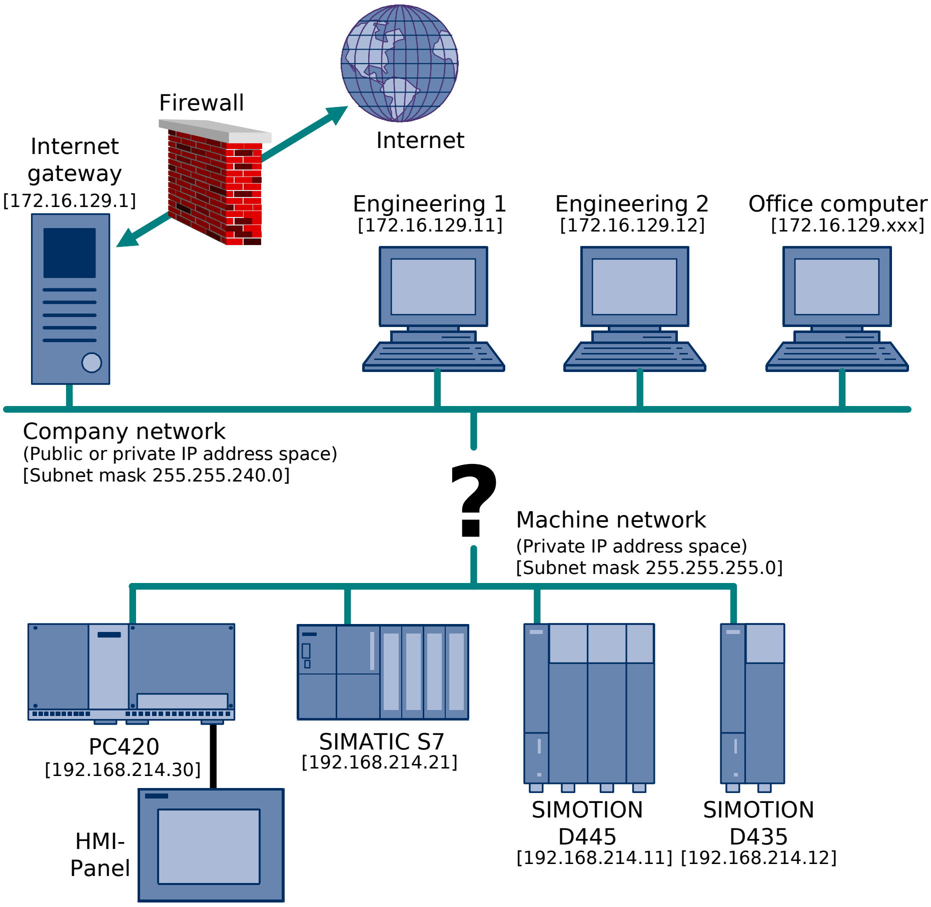
How do you connect a company network to a machine network under the aspect of high safety requirements?

Sample Configuration

A production machine is automated with several controllers. It is a combination of SIMATIC and SIMOTION controllers with subordinate SINAMICS drives technology. Machine operation is carried out on a PC420 (Microbox) with WinXP Embedded via OPC.

The individual controllers and the PC420 are networked to each other by means of Ethernet. The machine network is also used for the engineering.

Figure 1-1 Configuration of the company network and machine network



Requirements

The engineering computers are – amongst other computers – part of a company network (e.g. the machine manufacturer's). For reasons of safety and practicality the engineering should not

- be carried out in parallel directly on the machine network via a second network card,
- be carried out by re-plugging the Ethernet cables from company network to machine network and vice versa or re-parameterization of the Windows network settings.

However the machine should be connected to the company network. The engineering should be carried out via the company network down to the machine.

All services provided by the company network (Email, Intranet, Internet) should work for the engineering computers without any restrictions parallel to accessing the machine network.

This brings forth the following issues:

- Which components must be used for the connection of company and machine networks?
- How can an engineering computer which is linked to the company network access the machine network?
- How is it ascertained that only certain permitted engineering computers can access the machine network but not all other computers?
- How is it ascertained that devices from the machine network cannot randomly access the company network?
- How is it ascertained that only required services (such as STEP7 protocol services) are permitted to pass through the boundary between the company and machine networks?
- Which settings must be configured on the engineering computers and in the project?
  - for routing up to the drives components?
  - when several machines are connected to the company network in parallel, especially in the event of identical IP addresses in the individual machine networks?

2 Solution

The solution outlined in this chapter is based on the example described in chapter 1. This applies to both the HW configuration of the machine network and the IP addresses of the company and machine networks.

⚠ Attention

For use in your own application, the exemplary IP addresses, subnet masks… must be adapted to your actual conditions.

2.1 Component Selection

In order to connect a machine network to the company network you will need a network component which can handle routing and also has a firewall. The component used here is a SCALANCE S602.

The part number of the SCALANCE S602 is **6GK5602-0BA00-2AA3**.

For product information and manuals on the SCALANCE S602 please refer to Siemens A&D Product Support:

http://support.automation.siemens.com/WW/view/en/18701555/133400

The entire configuration of SCALANCE S602 is carried out using the ***Security Configuration Tool***.

2.2 Routing Settings of SCALANCE S602

Port 1 (P1 – External Network) is connected to the company network, and Port 2 (P2 – Internal Network) is connected to the machine network.

Port 1 receives IP address 172.16.130.30 from the IP address space of the company network. It is required to obtain clearance from the responsible IT-department for the company network which administers the IP addresses.

Port 2 receives IP address 169.168.214.40 from the IP address space of the machine network.

Note

When several machines are connected to the company network in parallel please ensure there is a unique IP address in the company network for each SCALANCE S602.

2.2.1 Initial installation of SCALANCE S602

Prior to the first download of SCALANCE S602 it must be ensured that its access point (IP address and subnet mask on Port 1) is set correctly for the ***Security Configuration Tool***.

1. Reset SCALANCE S602 to factory setting using the Reset key.

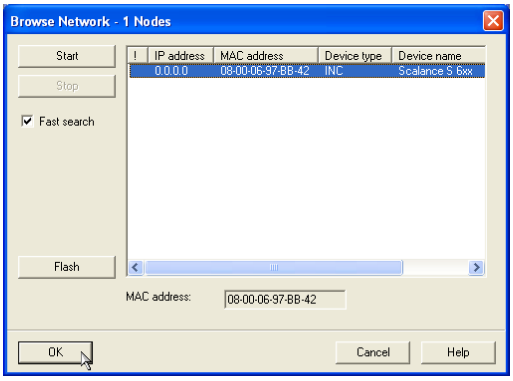
Note The reset key is located under the screw cap on the reverse side of the device. It must be pressed for several seconds until the fault LED is flashing yellow/red. The reset process lasts up to 2 minutes followed by the fault LED lighting continuous yellow.

2. Establish a point to point connection of the engineering computer using SCALANCE S602 on Port 1.

Note SCALANCE S has the auto crossing function, i.e. it is recognized whether the used cable has continuous or crossed send and receive lines.

3. Start the SIMATIC manager using menu command ***PLC*** ➔ Edit ***Ethernet Node…***. Select SCALANCE S602 via ***Browse...***. After reset to factory setting it has the IP address 0.0.0.0.

Figure 2-1 Find Ethernet node



Browse Network - 1 Nodes

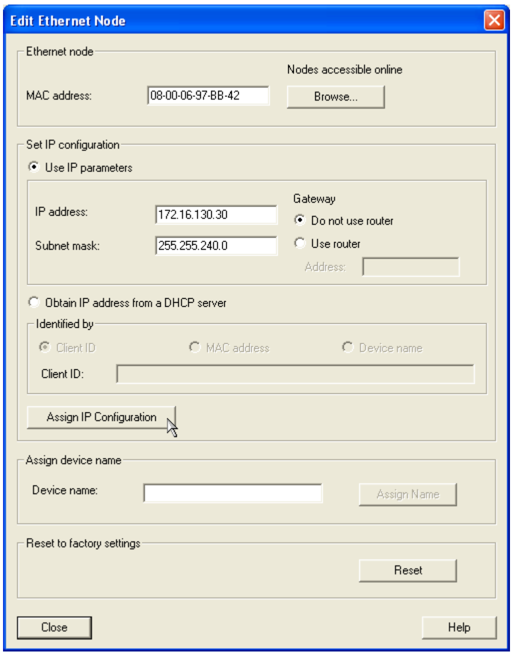
☑ Fast search

!	IP address	MAC address	Device type	Device name
	0.0.0.0	08-00-06-97-BB-42	INC	Scalance S 6xx

MAC address: 08-00-06-97-BB-42

4. The IP address and the subnet mask of Port 1 (P1 – External Network) are entered and assigned under ***Set IP configuration***.

Figure 2-2 First IP configuration of SCALANCE S602



MAC address: 08-00-06-97-BB-42

● Use IP parameters

IP address: 172.16.130.30

Subnet mask: 255.255.240.0

● Do not use router

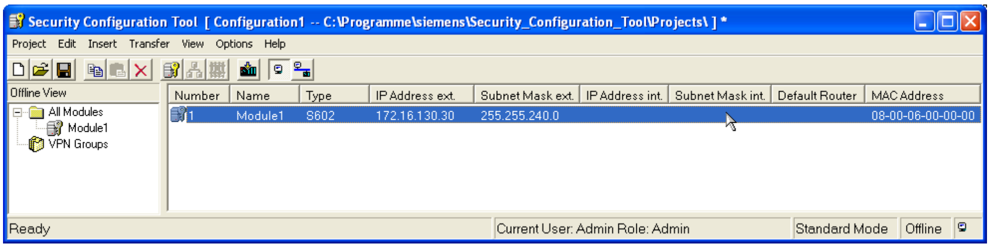
○ Use router

○ Obtain IP address from a DHCP server

2.2.2 Routing Configuration of SCALANCE S602

Use the ***Security Configuration Tool*** to generate a new project. The IP address and the subnet mask for the external network (company network) are assigned to the created module.

Figure 2-3 IP configuration of the external network

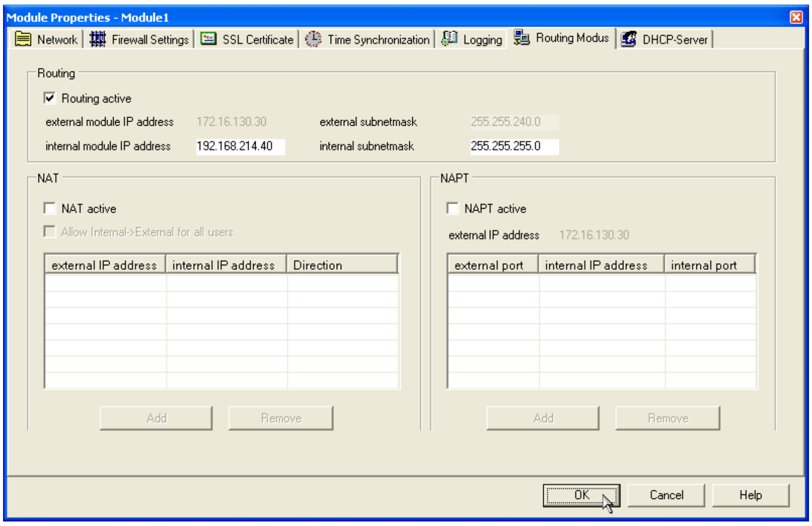

Security Configuration Tool [Configuration1 -- C:\Programme\siemens\Security_Configuration_Tool\Projects\ ] *
Project
Edit
Insert
Transfer
View
Options
Help
Offline View
All Modules
Module1
VPN Groups
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

Number	Name	Type	IP Address ext.	Subnet Mask ext.	IP Address int.	Subnet Mask int.	Default Router	MAC Address
1	Module1	S602	172.16.130.30	255.255.240.0				08-00-06-00-00-00

Use the command ***View → Advanced Mode*** to switch to advanced mode.

Use the context menu (or double click) to open the properties of the module. Tab ***Routing Modus*** activates the routing and assigns the IP address and subnet mask for the internal network (machine network).

Figure 2-4 Routing configuration and IP configuration of the internal network



Routing

☑ Routing active

external module IP address 172.16.130.30 external subnetmask 255.255.240.0

internal module IP address 192.168.214.40 internal subnetmask 255.255.255.0

NAT

□ NAT active

□ Allow Internal->External for all users

external IP address	internal IP address	Direction

NAPT

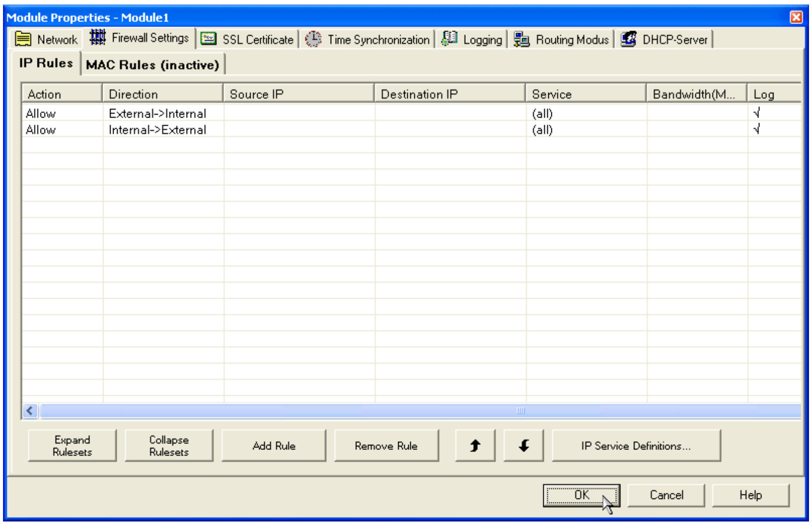
□ NAPT active

external IP address 172.16.130.30

external port	internal IP address	internal port

Use the ***Firewall Settings*** tab for the initial acceptance of services by all network nodes.

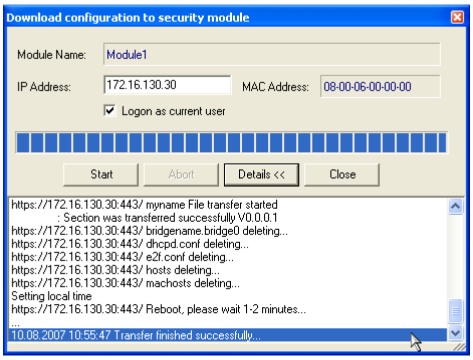
Figure 2-5 Configuration of the Firewall without restrictions



Action	Direction	Source IP	Destination IP	Service	Bandwidth(M...	Log
Allow	External->Internal			(all)		√
Allow	Internal->External			(all)		√

The settings are accepted, saved in the project and loaded onto SCALANCE S602.

Figure 2-6 Download of the configuration



Download configuration to security module

Module Name: Module1

IP Address: 172.16.130.30 MAC Address: 08-00-06-00-00-00

☑ Logon as current user

```
https://172.16.130.30:443/ myname File transfer started
              : Section was transferred successfully V0.0.0.1
https://172.16.130.30:443/ bridgename.bridge0 deleting...
https://172.16.130.30:443/ dhcpd.conf deleting...
https://172.16.130.30:443/ e2f.conf deleting...
https://172.16.130.30:443/ hosts deleting...
https://172.16.130.30:443/ machosts deleting...
Setting local time
https://172.16.130.30:443/ Reboot, please wait 1-2 minutes...
...
10.08.2007 10:55:47 Transfer finished successfully...
```

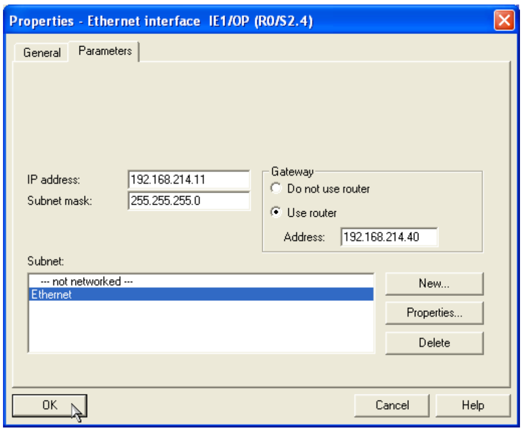
The basic routing mechanisms between the company and machine networks have now been installed.

2.3 Settings in the Project

For the individual controllers in the SIMOTION and SIMATIC projects it is required to specify the routing information.

This is achieved by defining the IP address of the router (SCALANCE S602) for the appropriate Ethernet interface in HW Config from the perspective of the machine network.

Figure 2-7 Configuration of the device Ethernet interface for SIMOTION D445



Properties - Ethernet interface IE1/OP (R0/S2.4)

IP address: 192.168.214.11

Subnet mask: 255.255.255.0

Gateway

○ Do not use router

● Use router

Address: 192.168.214.40

Subnet:

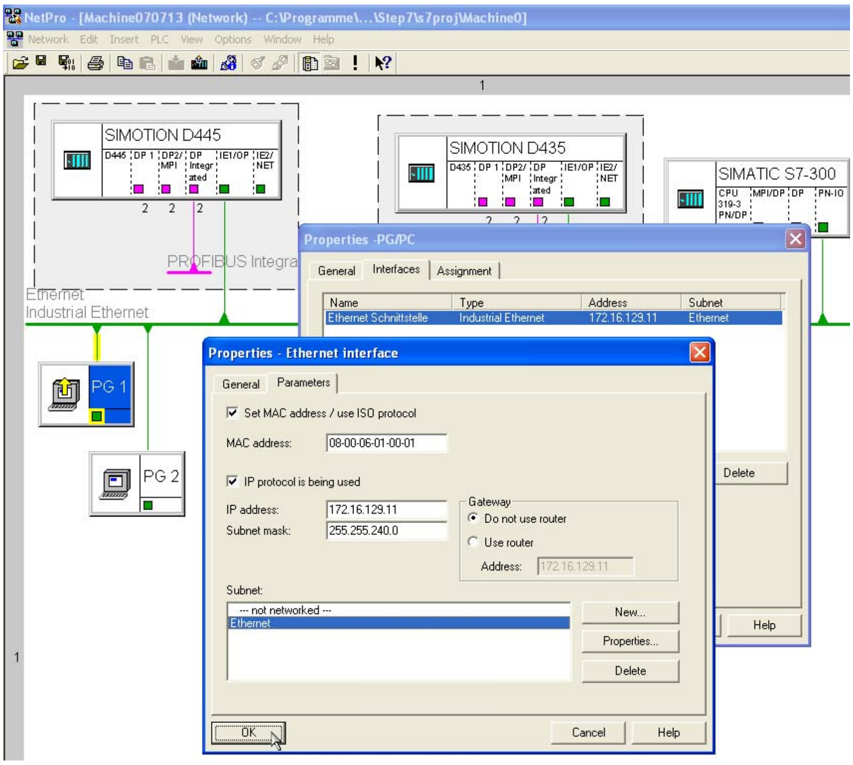
--- not networked ---

Ethernet

In addition to the controllers the PGs (engineering computers) must also be defined in NetPro. They receive their IP addresses from the company network in the Ethernet interface configuration.

The router does **not** need to be specified. These tasks are handled by the Windows routing settings of the engineering computers (see Chapter 2.4 Settings on the Engineering Computers).

Figure 2-8 PG Settings in NetPro


NetPro - [Machine070713 (Network) -- C:\Programme\...\Step7\s7proj\Machine0]
Network Edit Insert PLC View Options Window Help
1
SIMOTION D445
D445 DP 1 DP2/ MPI DP Integrated IE1/OP IE2/ NET
2 2 2
SIMOTION D435
D435 DP 1 DP2/ MPI DP Integrated IE1/OP IE2/ NET
2 2 2
SIMATIC S7-300
CPU 319-3 PN/DP MPI/DP DP PN-IO
PROFIBUS Integra
Ethernet
Industrial Ethernet
PG 1
PG 2
1

Properties -PG/PC

General | Interfaces | Assignment

Name	Type	Address	Subnet
Ethernet Schnittstelle	Industrial Ethernet	172.16.129.11	Ethernet

Delete

Help

Properties - Ethernet interface

General | Parameters

☑ Set MAC address / use ISO protocol

MAC address: 08-00-06-01-00-01

☑ IP protocol is being used

IP address: 172.16.129.11

Subnet mask: 255.255.240.0

Gateway

● Do not use router

○ Use router

Address: 172.16.129.11

Subnet:

--- not networked ---
Ethernet

New... | Properties... | Delete

OK | Cancel | Help

Conclusion

There is no unique information stored in the project.

The project is portable to other identical machines without change.

2.4 Settings on the Engineering Computers

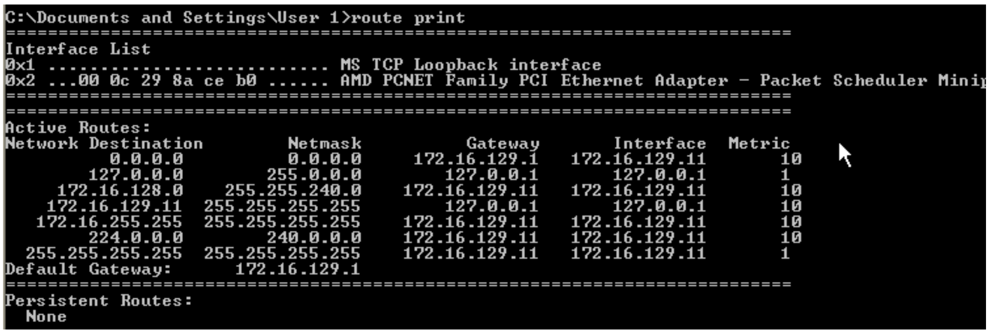
As a rule the entire IP configuration of a computer in a company network is assigned via a DHCP server. The DHCP-Server usually allocates IP addresses by means of their MAC address based on static allocation tables.

The standard gateway defined in the Windows IP properties defines the contact partner for IP packets which are not meant for its own subnet. The gateway, however, cannot use the IP packets which are meant for the machine network.

Therefore another route must be defined for IP packets with destination network 192.168.214.0. This is carried out, for instance, by using the prompt with the command ***route***.

Use the ***route print*** command to obtain a print out of the active routes.

Figure 2-9 Print out of active routes



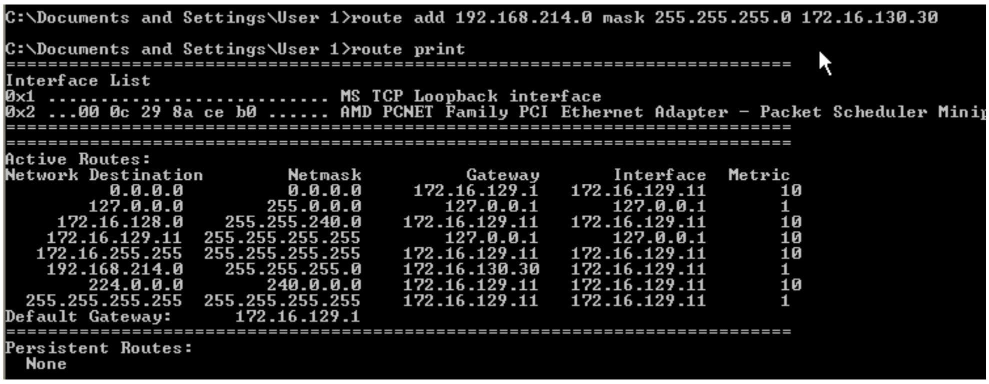
```
C:\Documents and Settings\User 1>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0c 29 8a ce b0 ...... AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Minip
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     172.16.129.1   172.16.129.11       10
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     172.16.128.0    255.255.240.0    172.16.129.11   172.16.129.11       10
    172.16.129.11  255.255.255.255        127.0.0.1       127.0.0.1       10
   172.16.255.255  255.255.255.255    172.16.129.11   172.16.129.11       10
        224.0.0.0        240.0.0.0    172.16.129.11   172.16.129.11       10
  255.255.255.255  255.255.255.255    172.16.129.11   172.16.129.11       1
Default Gateway:      172.16.129.1
===========================================================================
Persistent Routes:
  None
```

Use the ***route add <net address> mask <subnet mask> <router address>*** command to install an additional route.

- <net address> is the machine net address 192.168.214.0.
- <subnet mask> is the subnet mask of the machine network 255.255.255.0.
- <router address> is the company network address of the SCALANCE S602.

Check whether the route has been added successfully with a subsequent ***route print***.

Figure 2-10 Add Route

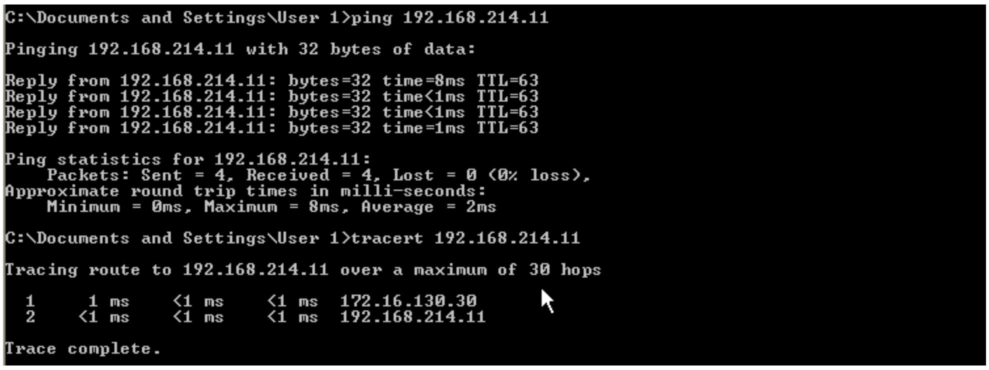


```
C:\Documents and Settings\User 1>route add 192.168.214.0 mask 255.255.255.0 172.16.130.30

C:\Documents and Settings\User 1>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0c 29 8a ce b0 ...... AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Minip
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     172.16.129.1   172.16.129.11       10
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     172.16.128.0    255.255.240.0    172.16.129.11   172.16.129.11       10
    172.16.129.11  255.255.255.255        127.0.0.1       127.0.0.1       10
   172.16.255.255  255.255.255.255    172.16.129.11   172.16.129.11       10
    192.168.214.0    255.255.255.0    172.16.130.30   172.16.129.11       1
        224.0.0.0        240.0.0.0    172.16.129.11   172.16.129.11       10
  255.255.255.255  255.255.255.255    172.16.129.11   172.16.129.11       1
Default Gateway:      172.16.129.1
===========================================================================
Persistent Routes:
  None
```

The destination devices can be addressed using the ***ping*** command with the firewall which is still deactivated. The ***tracert*** (trace route) command shows that the IP packets go their way via the IP address of the SCALANCE S602.

Figure 2-11 Test Route



```
C:\Documents and Settings\User 1>ping 192.168.214.11

Pinging 192.168.214.11 with 32 bytes of data:

Reply from 192.168.214.11: bytes=32 time=8ms TTL=63
Reply from 192.168.214.11: bytes=32 time<1ms TTL=63
Reply from 192.168.214.11: bytes=32 time<1ms TTL=63
Reply from 192.168.214.11: bytes=32 time=1ms TTL=63

Ping statistics for 192.168.214.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\Documents and Settings\User 1>tracert 192.168.214.11

Tracing route to 192.168.214.11 over a maximum of 30 hops

  1     1 ms    <1 ms    <1 ms  172.16.130.30
  2    <1 ms    <1 ms    <1 ms  192.168.214.11

Trace complete.
```

From now on the development tools SIMATIC Manager and SIMOTION Scout can be connected to the destination controllers without any restrictions.

2.4.1 Settings for Several Machine Networks

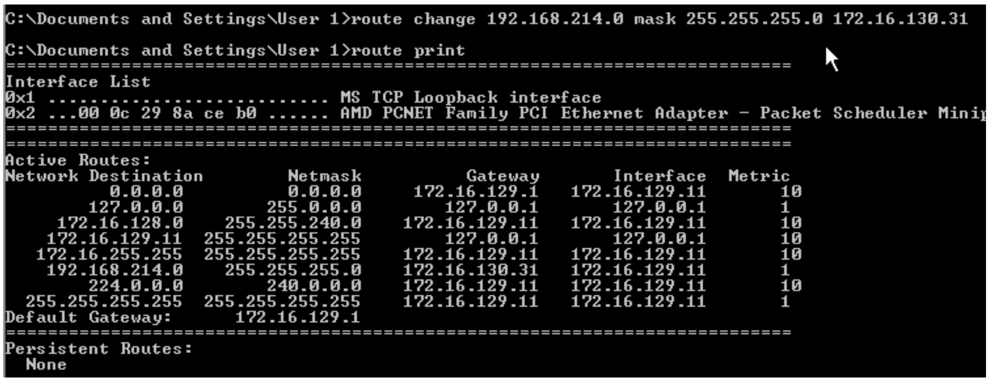
Several Machines with Different IP Address Spaces

When several machines with different IP address spaces should be reached, each route must be individually added by using ***route add***.

Several Machines with Identical IP Address Spaces

In order to switch between several machines with identical IP addresses, the route should be adapted in accordance with the required machine. If a route for the machine network has already been added, it is changed using the ***route change*** command.

Figure 2-12 Change Route



```
C:\Documents and Settings\User 1>route change 192.168.214.0 mask 255.255.255.0 172.16.130.31

C:\Documents and Settings\User 1>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0c 29 8a ce b0 ...... AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Minip
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.129.1   172.16.129.11       10
        127.0.0.0        255.0.0.0         127.0.0.1       127.0.0.1       1
     172.16.128.0    255.255.240.0     172.16.129.11   172.16.129.11       10
    172.16.129.11  255.255.255.255         127.0.0.1       127.0.0.1       10
   172.16.255.255  255.255.255.255     172.16.129.11   172.16.129.11       10
    192.168.214.0    255.255.255.0     172.16.130.31   172.16.129.11       1
        224.0.0.0        240.0.0.0     172.16.129.11   172.16.129.11       10
  255.255.255.255  255.255.255.255     172.16.129.11   172.16.129.11       1
Default Gateway:      172.16.129.1
===========================================================================
Persistent Routes:
  None
```

Note The commands listed in this chapter can also be automated easily by using batch commands or scripts.

2.5 Firewall Settings of SCALANCE S602

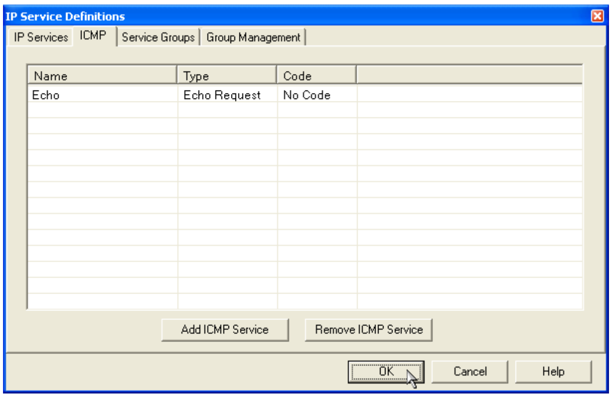
Before setting the firewall ask yourself the following question: “Exactly which services do I need?“. The list below may give you some reference points.

- The Ping command should work on all existing devices in the machine network.
- All required services for the SIEMENS development tools SIMATIC Manager and SIMOTION Scout incl. integrated STARTER.
- Access to network shares on the PC420.
- The permitted services may only be initiated by defined computers.

The protocols and services are defined in the properties of the module in the ***Firewall Settings*** via ***IP Service Definitions...***.tab.

For the ***ping*** command you will be the ICMP service ***Echo Request***.

Figure 2-13 Definition of ICMP Services

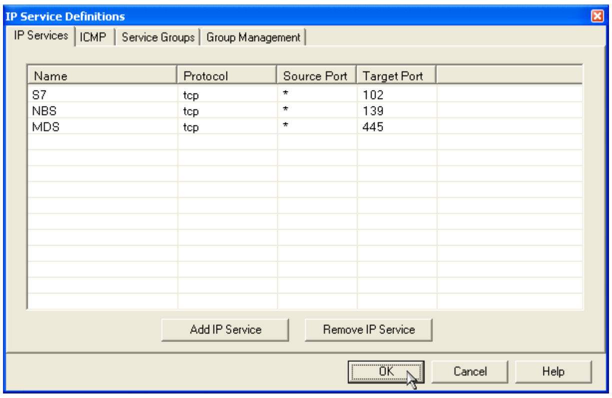


Name	Type	Code
Echo	Echo Request	No Code

For the S7 services you will need the destination port 102 with the TCP protocol.

Access to Windows network shares works are transacted over NetBIOS Services (TCP-Port 139) and Microsoft Directory Services (TCP-Port 445).

Figure 2-14 Definition of IP Services

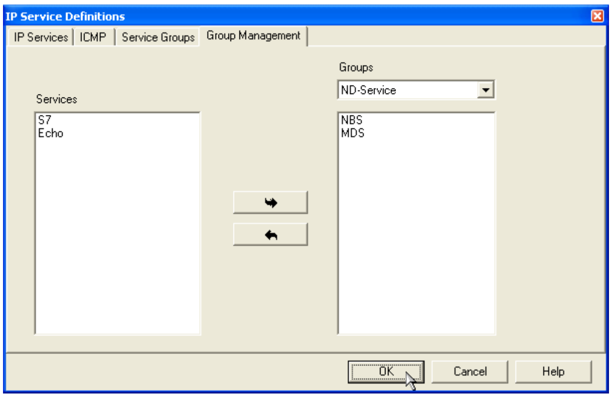


Name	Protocol	Source Port	Target Port
S7	tcp	*	102
NBS	tcp	*	139
MDS	tcp	*	445

Subject to change without prior notice.

Groups can be defined under the ***Service Groups*** tabs. The individual services are assigned to the groups in the ***Group Management*** tab. In this precise example the network services are compiled in the group ND-Service (network drives).

Figure 2-15 Group Management of network drives



Groups: ND-Service

Services	Groups
S7	NBS
Echo	MDS

Use the services now defined here to formulate the IP rules with the permitted source and destination IP addresses and address spaces.

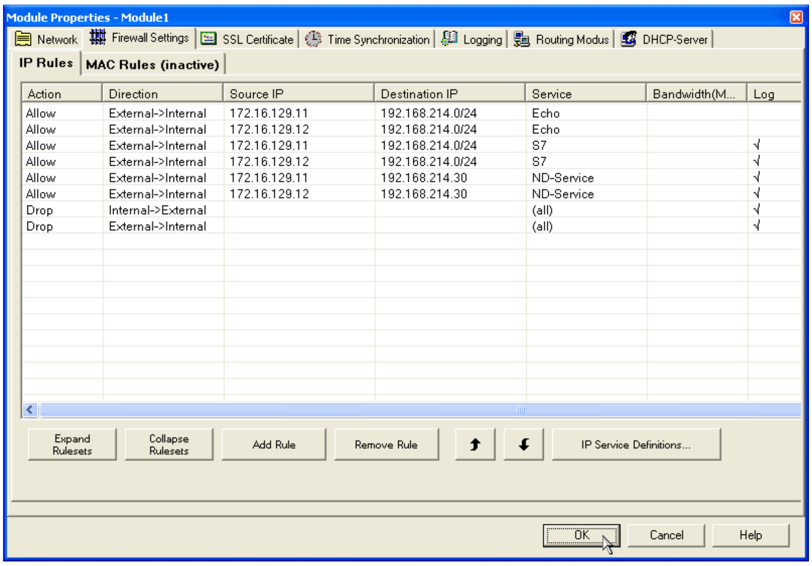
Note

> The direction indicator ***External->Internal*** always permits the corresponding reply messages in the opposite direction.

Enter the permitted engineering computers as the source IP address. For the services Echo and S7 use all network nodes as the destination address. The network services are only permitted to PC420 with its specific IP address.

All other services of any other network nodes are rejected.

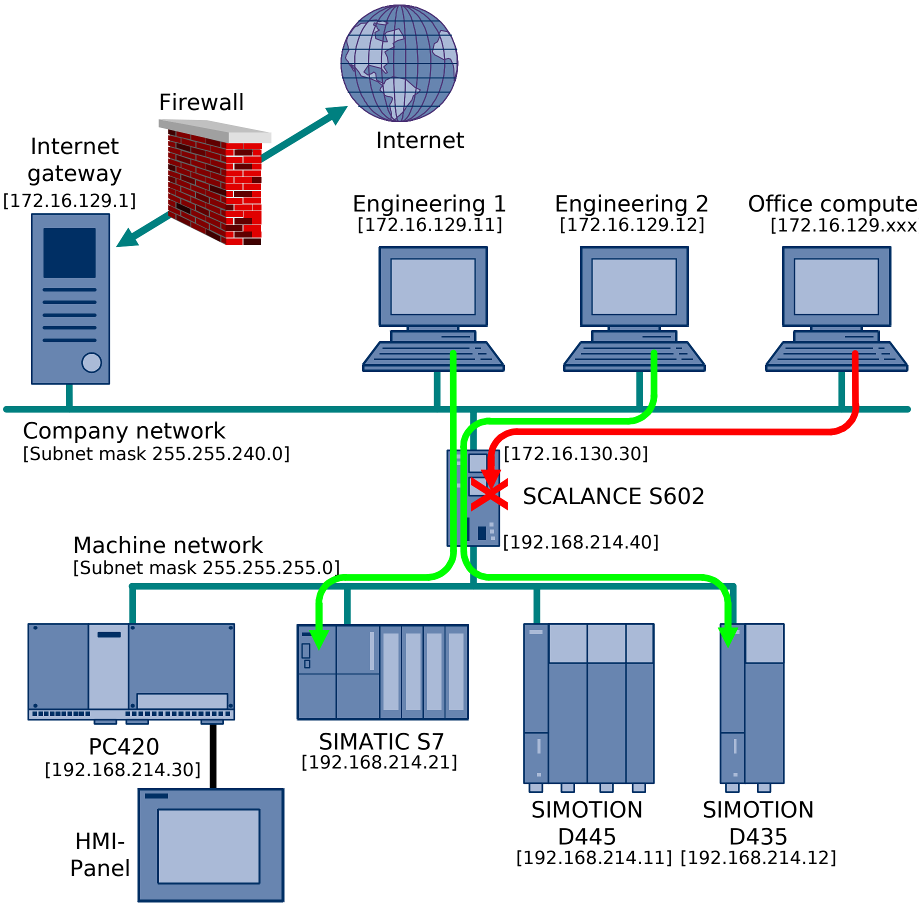
Figure 2-16 Definition of IP Rules



Action	Direction	Source IP	Destination IP	Service	Bandwidth(M...	Log
Allow	External->Internal	172.16.129.11	192.168.214.0/24	Echo		
Allow	External->Internal	172.16.129.12	192.168.214.0/24	Echo		
Allow	External->Internal	172.16.129.11	192.168.214.0/24	S7		√
Allow	External->Internal	172.16.129.12	192.168.214.0/24	S7		√
Allow	External->Internal	172.16.129.11	192.168.214.30	ND-Service		√
Allow	External->Internal	172.16.129.12	192.168.214.30	ND-Service		√
Drop	Internal->External			(all)		√
Drop	External->Internal			(all)		√

2.6 Ultimate Layout with SCALANCE S602

Figure 2-17 Configuration of the company network and machine network



3 Appendix

3.1 Identification of Protocols and Ports of Required Services

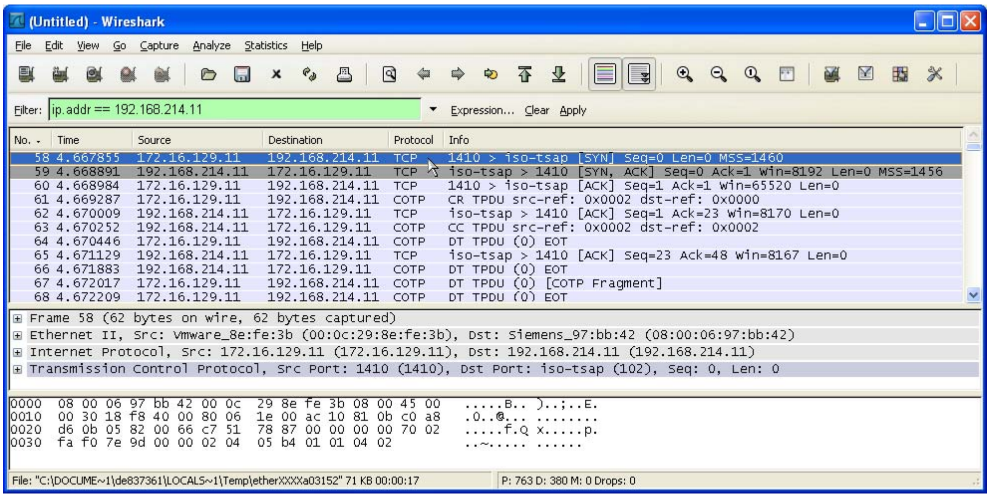
When the protocol and port numbers of a required service are unknown, the required information can be obtained via a network sniffer. We recommend the open source program ***WireShark***.

http://www.wireshark.org/

Procedure:

1. SCALANCE S602 is used as a router only without firewall – all services are enabled.
2. The network sniffer is started on the local engineering computer and records the incoming and outgoing data traffic.
3. The required service is started – e.g. ping command is called or go online with SIMOTION Scout on a controller.
4. The network sniffer is stopped and the recorded data traffic is surrounded by means of filter criteria. This is how you can indicate only those data packages, for instance, which have specific source and destination IP addresses.
5. As a rule you can quickly establish from the selected data traffic which protocol (ICMP, UDP, TCP) and which port are relevant.
6. The protocol and the required service are defined and are enabled in the Firewall. A final test of the service confirms that the defined rules apply.

Figure 3-1 Filtered data traffic from and to IP address 192.168.214.11



Filter: ip.addr == 192.168.214.11

```
No. -  Time       Source           Destination      Protocol  Info
  58 4.667855   172.16.129.11    192.168.214.11   TCP       1410 > iso-tsap [SYN] Seq=0 Len=0 MSS=1460
  59 4.668891   192.168.214.11   172.16.129.11    TCP       iso-tsap > 1410 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456
  60 4.668984   172.16.129.11    192.168.214.11   TCP       1410 > iso-tsap [ACK] Seq=1 Ack=1 Win=65520 Len=0
  61 4.669287   172.16.129.11    192.168.214.11   COTP      CR TPDU src-ref: 0x0002 dst-ref: 0x0000
  62 4.670009   192.168.214.11   172.16.129.11    TCP       iso-tsap > 1410 [ACK] Seq=1 Ack=23 Win=8170 Len=0
  63 4.670252   192.168.214.11   172.16.129.11    COTP      CC TPDU src-ref: 0x0002 dst-ref: 0x0002
  64 4.670446   172.16.129.11    192.168.214.11   COTP      DT TPDU (0) EOT
  65 4.671129   192.168.214.11   172.16.129.11    TCP       iso-tsap > 1410 [ACK] Seq=23 Ack=48 Win=8167 Len=0
  66 4.671883   192.168.214.11   172.16.129.11    COTP      DT TPDU (0) EOT
  67 4.672017   172.16.129.11    192.168.214.11   COTP      DT TPDU (0) [COTP Fragment]
  68 4.672209   172.16.129.11    192.168.214.11   COTP      DT TPDU (0) EOT
```

```
⊞ Frame 58 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Vmware_8e:fe:3b (00:0c:29:8e:fe:3b), Dst: Siemens_97:bb:42 (08:00:06:97:bb:42)
⊞ Internet Protocol, Src: 172.16.129.11 (172.16.129.11), Dst: 192.168.214.11 (192.168.214.11)
⊞ Transmission Control Protocol, Src Port: 1410 (1410), Dst Port: iso-tsap (102), Seq: 0, Len: 0
```

```
0000  08 00 06 97 bb 42 00 0c  29 8e fe 3b 08 00 45 00   .....B.. )..;..E.
0010  00 30 18 f8 40 00 80 06  1e 00 ac 10 81 0b c0 a8   .0..@... ........
0020  d6 0b 05 82 00 66 c7 51  78 87 00 00 00 00 70 02   .....f.Q x.....p.
0030  fa f0 7e 9d 00 00 02 04  05 b4 01 01 04 02         ..~..... ......
```

File: "C:\DOCUME~1\de837361\LOCALS~1\Temp\etherXXXXa03152" 71 KB 00:00:17 | P: 763 D: 380 M: 0 Drops: 0

From the illustration above you can deduct that S7 services always run on the controller via Port 102.

For TCP protocols it is easiest to analyze the established connection of the sequence SYN – SYN, ACK – ACK. As a rule the essential port is that of the TCP server. The TCP server is the passive node when the connection is established.

Note S7 services based on TCP/IP are always transacted via Port 102 (ISO-TSAP service).

Note For a list of all usual ports with their associated services please refer to http://www.iana.org/assignments/port-numbers.

Subject to change without prior notice.